Федеральное государственное автономное образовательное учреждение высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
Факультет информационных технологий
Кафедра «Информационная безопасность»
Направление подготовки/ специальность: 10.05.03 Информационная безопасность автоматизированных систем

ОТЧЕТ

по проектной практике

Студент: Ермаков Михаил Андреевич Группа: 241-371
Место прохождения практики: Московский Политех, кафедра «Информационная безопасность»

Отчет принят с оценкой _____ Дата _____
Руководитель практики: _____

Москва 2025

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В рамках проектной практики была выполнена работа, направленная на приобретение и закрепление профессиональных компетенций в области информационных технологий, а также на изучение современных подходов к разработке и обеспечению безопасности веб-приложений. Практика состояла из двух частей: базовой и вариативной, каждая из которых включала теоретическое и практическое освоение ключевых аспектов IT-сферы.

В базовой части практики основное внимание было уделено созданию статического веб-сайта с использованием генератора Hugo. На сайте была размещена информация о проекте, выполняемом в рамках дисциплины «Проектная деятельность». Кроме того, в ходе практики состоялось участие в мастер-классе от компании «Инфосистемы Джет» на тему «Как развиваться в ИБ», что стало опытом, продемонстрировавшим реальные механизмы принятия решений в сфере информационной безопасности.

Вариативная часть практики была посвящена исследованию методик тестирования защищенности веб-приложений. В рамках этого задания проведен анализ современных подходов, инструментов и стандартов, применяемых для выявления уязвимостей в веб-приложениях. Изучение данной темы способствовало углублению понимания принципов кибербезопасности и методов обеспечения защиты цифровых решений.

Выполненные работы позволили не только развить технические навыки, но и расширить кругозор в области веб-разработки и информационной безопасности.

1. Основная информация о проекте

1. Название проекта:

Помощь людям с ОВЗ: сайт для оказания экстренной помощи

2.Цели и задачи проекта:

Данный раздел определяет цели и задачи проекта и его исследовательской части, а также объект и предмет. Цель проекта – это конечный результат, которую команда проекта хочет достичь в ходе выполнения проекта. Исходя из целей проекта, формируются его задачи, которые существуют для того, чтобы дать наводку на действия для достижения целей. Важное уточнение: в данном контексте, задачи появляются по мере разработки, поэтому здесь задачи описаны в рамках первой аттестации. Ниже представлены такие понятия как «объект» и «предмет» проекта. Объект представляет собой изучаемое, предмет подразумевает за собой свойство изучаемого.

Объект проекта: Сайт для помощи людям с ОВЗ и инвалидам.

Предмет проекта: Разработка сайта для помощи людям с ОВЗ и инвалидам «Поддержка рядом».

Цель проекта:

- Создание сайта для взаимодействия волонтеров и лиц с ОВЗ в одном из административных округов г. Москва.

Задачи:

- Создание дизайна главных страниц.
- Разработка интерактивных элементов для главной страницы.
- Верстка сайта.
- Создание базы данных
- Создание политики конфиденциальности
- Адаптация сайта под мобильные устройства
- Запустить продвижение сайта в соцсетях
- Составление диаграммы Ганта
- Составление проектно-технической документации

- Подготовка презентации к защите проекта
- Защита проекта

2. Общая характеристика деятельности организации

1. Наименование заказчика:

Московский Политехнический университет

2. Организационная структура:

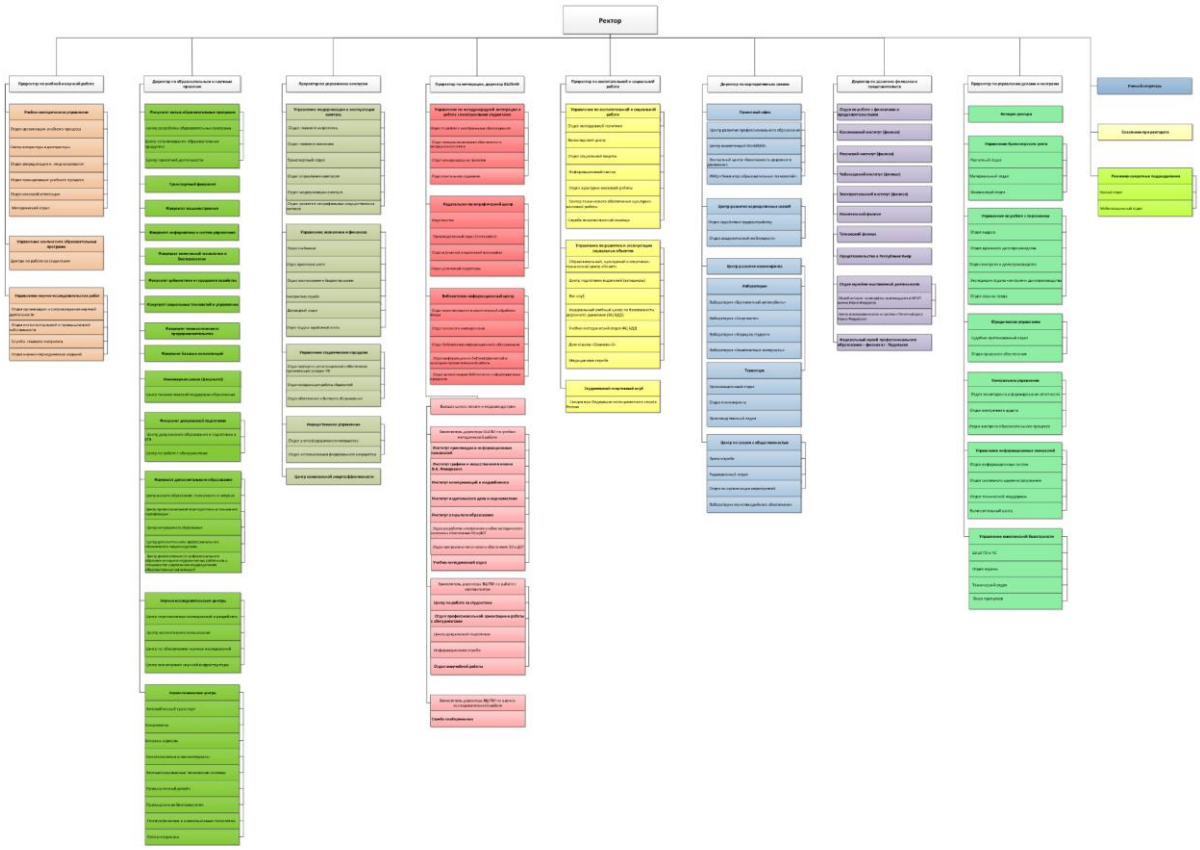

Рисунок 1 – Организационная структура организации «Московский политехнический университет»

3. Описание деятельности:

Московский политехнический университет – это ведущее образовательное и научное учреждение, сочетающее традиции академического мастерства с инновационными подходами в подготовке высококвалифицированных специалистов для высокотехнологичных отраслей экономики. Университет осуществляет многопрофильную деятельность, включающую образовательные программы бакалавриата, специалитета, магистратуры и аспирантуры по направлениям, связанным с инженерией, IT, робототехникой, энергетикой, транспортом, биотехнологиями и другими ключевыми областями современной науки и промышленности. Вуз активно

развивает прикладные исследования, сотрудничая с крупнейшими корпорациями и научными центрами, что позволяет студентам и преподавателям участвовать в реальных проектах, направленных на решение актуальных технологических и социально-экономических задач. Московский политехнический университет уделяет особое внимание интеграции образования, науки и производства, внедряя междисциплинарные подходы и современные методики обучения, включая цифровые технологии и проектно-ориентированное образование. Университет также является площадкой для развития предпринимательских инициатив, поддерживая стартапы и инновационные разработки своих студентов и сотрудников. Среди приоритетных направлений деятельности – международное сотрудничество, участие в глобальных научных и образовательных программах, а также подготовка кадров, способных конкурировать на мировом уровне. Московский политехнический университет стремится к формированию новой генерации инженеров, ученых и управленцев, готовых к вызовам быстро меняющегося технологического ландшафта.

3. Описание задания по проектной практике

1. Базовая часть задания

В ходе выполнения базовой части проектной практики была проделана значительная работа по освоению современных инструментов разработки и документирования. Практика началась с создания группового репозитория на платформе GitHub, где в дальнейшем хранились все материалы проекта. Для работы с репозиторием потребовалось детальное изучение системы контроля версий Git. В процессе обучения были освоены ключевые команды: клонирование существующего репозитория (git clone), создание новых веток для параллельной разработки (git branch), переключение между ветками (git checkout), а также фиксация изменений с комментариями (git commit) и отправка обновлений на удаленный сервер (git push).

Особое внимание было уделено оформлению проектной документации. Для этого потребовалось изучить синтаксис языка разметки Markdown, который впоследствии использовался для создания всех текстовых материалов проекта. В Markdown-формате были подготовлены: подробное описание проекта с указанием его целей и задач, отчеты о проделанной работе, а также документация. Все эти материалы были систематизированы и размещены в соответствующем разделе Git-репозитория.

Важной частью практики стала разработка статического веб-сайта. После анализа доступных технологий был выбран генератор статических сайтов Hugo, который значительно упростил процесс создания и поддержки веб-ресурса. Созданный сайт посвящен проекту по дисциплине «Проектная деятельность» и содержит несколько обязательных разделов. На главной странице размещена краткая аннотация проекта, позволяющая пользователям быстро ознакомиться с его сутью. Раздел «О проекте» содержит детальное описание целей, задач и актуальности работы. Страница «Участники» включает информацию обо всех членах проекта с указанием их личного вклада в проект. Особое внимание было уделено разделу «Журнал», где публиковались записи о ходе работы, включая описание выполненных задач.

Также на сайте создан раздел «Ресурсы» с полезными ссылками на дополнительные материалы. Для улучшения визуального восприятия некоторые разделы сайта были дополнены соответствующими графическими элементами.

Значимым этапом практики стало участие в мастер-классе компании «Инфосистемы Джет» на тему «Как развиваться в ИБ». Участники моделировали построение защищённой информационной системы с бюджетом 200 джеткоинов. Необходимо было выбрать меры защиты из трёх категорий: технические мероприятия, персонал и организационные мероприятия. Каждая мера имела стоимость и оценку эффективности в баллах защиты. Главная задача — достичь максимальной защищённости в рамках выделенного бюджета. В процессе участники анализировали варианты, сравнивали их эффективность, расставляли приоритеты и формировали итоговую конфигурацию системы.

В результате выполнения всех перечисленных задач были получены практические навыки работы с современными инструментами разработки, освоены принципы командной работы над проектом, а также приобретен ценный опыт взаимодействия с профессиональным сообществом. Все поставленные задачи были выполнены в полном объеме и в установленные сроки.

2. Вариативная часть

Индивидуальное кафедральное задание разработано с целью развития профессиональных компетенций, соответствующих направлению «Информационная безопасность автоматизированных систем»

Тема: «Анализ методик тестирования защищенности веб-приложений»

Поставленные задачи:

1. Классифицировать методы тестирования защищенности веб-приложений.
2. Рассмотреть основные уязвимости и методы их выявления.

3. Сравнить инструменты и подходы к тестированию.

4. Проанализировать методологии и стандарты тестирования (OWASP, PTES, NIST, ISO).

5. Изучить практические аспекты тестирования, включая этапы, особенности API-тестирования и юридические аспекты.

6. Оценить эффективность различных методик (автоматизированные vs ручные, ложные срабатывания, метрики безопасности).

7. Разработать рекомендации по выбору подходов в зависимости от типа приложения, ресурсов команды и регуляторных требований.

4. Описание достигнутых результатов по проектной практике

В ходе выполнения **базовой части** мной были достигнуты следующие результаты:

1. Был создан и настроен Git-репозиторий, также были изучены базовые команды Git. **Затраченное время: 5 часов**
2. Был изучен синтаксис языка Markdown, а также написаны документы с его использованием. **Затраченное время: 5 часов**
3. Был изучен функционал генератора статических веб-сайтов Hugo. Запущен веб-сайт и добавлены разделы «Участники», «Журнал», далее эти разделы были наполнены материалами проекта в рамках дисциплины «Проектная деятельность». Также было изменено лого сайта. **Затраченное время: 22 часа**
4. Было посещено мероприятие организации-партнера от компании «Инфосистемы Джет» на тему «Как развиваться в ИБ» и написан отчет по данному мероприятию в формате Markdown, и загружен в репозиторий и на сайт. **Затраченное время: 8 часов**

В ходе выполнения **вариативной части** мной были достигнуты следующие результаты:

1. Рассмотрение основных уязвимостей и методов их выявления. Изучены наиболее распространенные уязвимости веб-приложений (SQL-инъекции, XSS, IDOR, небезопасная аутентификация, уязвимые зависимости и др.). Проанализированы методы их обнаружения, включая инструментальные (Burp Suite, SQLmap) и ручные техники тестирования. **Затрачено времени: 12 часов**
2. Анализ методологий и стандартов тестирования (OWASP, PTES, NIST, ISO). Изучены ключевые стандарты и руководства (OWASP Testing Guide, PTES, NIST SP 800-115, ISO/IEC 27001 и 27034). Определены их основные принципы, этапы тестирования и рекомендации по внедрению в процессы разработки и аудита безопасности. **Затрачено времени: 8 часов**

3. Оценка эффективности различных методик

Проведен анализ преимуществ и недостатков автоматизированного и ручного тестирования, рассмотрены проблемы ложных срабатываний и пропущенных уязвимостей. Изучены метрики оценки безопасности (CVSS, Risk Rating) для объективного измерения уровня защищенности. **Затрачено времени: 7 часов**

4. Разработка рекомендаций по выбору подходов

На основе проведенного анализа сформулированы рекомендации по выбору методов тестирования в зависимости от типа приложения (публичное/внутреннее), доступных ресурсов команды и регуляторных требований (PCI DSS, ГОСТ). Определена важность комбинированного подхода (автоматизация + ручное тестирование) для максимального охвата угроз. **Затрачено времени: 5 часов**

ЗАКЛЮЧЕНИЕ

В ходе практики были успешно выполнены все поставленные задачи, как в базовой, так и в вариативной части. Освоены ключевые навыки: работа с Git, разработка и публикация сайта на Hugo, взаимодействие с карьерными марафоном, а также оформление технической документации. Особую ценность представило практическое занятие от компании «Инфосистемы Джет», где удалось применить стратегический подход к построению системы информационной безопасности в условиях ограниченных ресурсов.

Главным результатом стало индивидуальное задание. Проведенное исследование позволило систематизировать ключевые методы тестирования безопасности веб-приложений и выработать практические рекомендации по их применению. Полученные результаты подтверждают необходимость комплексного подхода, сочетающего автоматизированные инструменты с ручным тестированием для обеспечения надежной защиты.

Полученный опыт и результаты создают надёжную основу для дальнейшего профессионального роста в области ИБ и будущей проектной деятельности.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. OWASP Web security testing guide // Owasp URL: https://owasp.org/www-project-web-security-testing-guide/ (дата обращения: 10.05.2025).
2. SP 800-115, Technical Guide to Information Security Testing and Assessment // Nist URL: https://csrc.nist.gov/pubs/sp/800/115/final (дата обращения: 15.05.2025).
3. The Penetration Testing Execution Standart // Pentest-standart URL: http://www.pentest-standard.org/index.php/Main_Page (дата обращения: 15.05.2025).
4. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. – Международный стандарт. – 2022. – 44 с.
5. ISO/IEC 27034-1:2011 Information technology — Security techniques — Application security — Part 1: Overview and concepts. – Международный стандарт. – 2011. – 32 с.
6. ГОСТ Р 7.0.100-2018. Библиографическая запись. Библиографическое описание. Общие требования и правила составления : национальный стандарт Российской Федерации. – Введ. 2019-07-01. – Москва : Стандартинформ, 2018. – 124 с.
7. Hugo Static Site Generator : [сайт]. – URL: https://gohugo.io (дата обращения: 15.05.2025).